Judge Robart

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. VOLODYMYR KVASHUK, Defendant.	NO. CR19-143JLR RESPONSE TO MOTION TO REVOKE DETENTION ORDER

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Michael Dion, Assistant United States Attorney, files this redacted, unsealed response to Defendant Volodymyr Kvashuk's motion to revoke Magistrate Judge Theiler's detention order. For the reasons set forth below, the Court should deny the motion.[1]

I. SUMMARY

Magistrate Judge Theiler detained Kvashuk because she found that he was a danger and a risk of flight. Kvashuk, a former Microsoft employee, is charged with embezzling $10 million from the company. He faces a long sentence if convicted, and the evidence is powerful. Indeed, the evidence is even stronger than it was when

[1] [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Theiler issued her detention order. Since then, investigators found "smoking gun" evidence on a thumb drive seized from Kvashuk's house.

Kvashuk is a Ukrainian citizen who does not have permanent status in the United States. The Ukraine does not allow extradition of its citizens – the Ukrainian constitution specifically forbids it. Kvashuk, who faces a long prison sentence in this case, has great incentive to return to his home country – where his family lives, where he has spent most of his life, and where he would be beyond the reach of U.S. law enforcement.

Furthermore, Kvashuk may well have the means to flee. Kvashuk stole $10 million in digital currency. Law enforcement has only identified about $2.8 million in proceeds. Kvashuk is a sophisticated user of cryptocurrency who has taken steps to conceal the money trail from his crime. Although Kvashuk likely resold the digital currency at a discount, he may well still have millions in proceeds hidden somewhere. Indeed, agents found a note in his house outlining his plans to spend "ten million dollars," as well as evidence of accounts and bitcoin wallets that may hold additional proceeds.

Although counsel assures the Court that Kvashuk has no other assets, Kvashuk himself refused to verify that. Kvashuk did not make a meaningful financial disclosure to Pretrial Services. He refused to say how he paid cash for a $160,000 Tesla and a $1.6 million waterfront home. He refused to say whether he had other cryptocurrency accounts.

Given these facts, there are no conditions of release that can adequately address the risk of flight.

II. FACTS

A. Kvashuk's Background and Immigration Status

Kvashuk is a twenty-five year old Ukrainian software engineer. He was born in Rivne, where his father still lives and teaches at the National University of Ostroh Academy. Kvashuk earned a Bachelor's and Master's degrees in Economics and Cybernetics from that University in 2015.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Kvashuk arrived in the United States on a temporary B-2 visa in April 2015. The defense states that Mr. Kvashuk applied for asylum on June 19, 2015. Since his arrival, he has worked at several tech companies in various roles related to software engineering. He began work for Microsoft Corporation ("Microsoft") through a vendor from August 2016 to October 2017. Microsoft hired him as an employee in December 2017. In June 2018, the company uncovered the fraud and fired Kvashuk.

Although Kvashuk has no permanent status in the United States, the defense has noted that he is permitted to live and work in this country pending a ruling on his asylum petition.

B. Kvashuk's $10 Million Embezzlement Scheme

As explained below, Kvashuk used his position as a member of the Microsoft team that tested the company's online store to steal $10 million from the company.[2]

Background of the testing program

Microsoft offers products and services to the public via its online store. To order from the store, a customer must create an account and link the account to (1) an email address, and (2) a credit card or other payment instrument.

The testing program was designed to simulate the experience of a customer trying to order products or services from the Microsoft online store. Testers would set up a test store account, which would be linked to a test email account and a fake credit card. The group that ran the testing, the Universal Store Team or "UST" team, would "whitelist" the test account, meaning that the account would bypass the company's normal security protections and data retention protocols.

Kvashuk's scheme exploited a vulnerability in the testing program. The program was set up to ensure that no physical goods would be delivered when orders were placed by test accounts, but there was no safeguard to prevent the delivery of digital currency ("currency stored value" or CSV), such as digital gift cards. A tester could use a test

[2] Additional details are in the Complaint of Special Agent Michael Spiess, attached as Exhibit 1.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

account to order CSV, and would get a code that could be redeemed and used to buy products or services from the Microsoft store.

Kvashuk discovered this flaw and launched his scheme. At first, Kvashuk used his own test account to steal relatively small amounts of CSV. Eventually, Kvashuk expanded his scheme, and used accounts belonging to other testers to steal $10 million in CSV.

Kvashuk's Early Thefts Using His Own Test Account

The test account that MS set up for Kvashuk was called the "vokvas" test account. Kvashuk used the vokvas account to steal about $12,000 during the early phase of his scheme, from April to October of 2017. Although Kvashuk used his own test account to purchase the CSV, he generally used store accounts that were not in his name to redeem the CSV and make purchases from the Microsoft store. In one case, for example, Kvashuk appears to have used CSV to purchase products under the alias "Grigor Shikor." Kvashuk made these purchases using Microsoft store accounts linked to the email addresses pikimajado@tinoza.org and xidijenizo@axsup.net. The "pikimajado" and "xidijenizo" email accounts were temporary, disposable accounts set up with service providers that typically do not preserve subscriber information.

Microsoft investigators interviewed Kvashuk in May of 2018. Kvashuk admitted to using his test account to purchase CSV, and also admitted to using that CSV to purchase (or attempt to purchase) some products. Kvashuk claimed that he was not given clear instructions about what he could and could not purchase with his test account, and said that that he thought it was permissible to take CSV because it is not "real money." Kvashuk denied using test accounts for large-scale CSV purchases.

Expansion of the Scheme Via Other Testers' Accounts

When Kvashuk first joined the testing team, he was working for a Microsoft contractor. His contracting job ended on October 1, 2017. Microsoft hired him as a direct employee (again on the testing team) on December 1, 2017.

Shortly before he joined Microsoft as a direct employee, Kvashuk ramped up the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

scale of the fraud and took new steps to hide his identity.

Starting on November 26, 2017, Kvashuk stopped using his own test account to purchase CSV, and began using accounts belonging to other testers. In particular, Kvashuk used the mstest_avestu@outlook.com and the mstest_sfwe2eauto@outlook.com test accounts (the "avestu" and "sfwe2eauto" accounts) to purchase the bulk of the CSV. He continued using other testers' accounts until March 23, 2018, and stole about $10 million during that time.

Kvashuk knew that, although he was using other testers' accounts, his IP address, device ID, and other data might lead investigators to him. His internet search history shows that Kvashuk researched ways to anonymize himself online. Kvashuk used IP proxy services that concealed his true IP address when logging into the other testers' accounts. Records show that Kvashuk used these same proxy services to log into his personal email account and his Coinbase cryptocurrency account.

Unexplained Wealth

At least some of the stolen CSV was resold on overseas reseller websites to third parties. Investigators have not yet been able to get records from these sites. However, CSV sold on these reseller sites was traced back to CSV stolen from Microsoft. Records of Kvashuk's Internet search history show that – only days before Kvashuk began buying CSV in other testers' names – Kvashuk was researching how to sell CSV online.

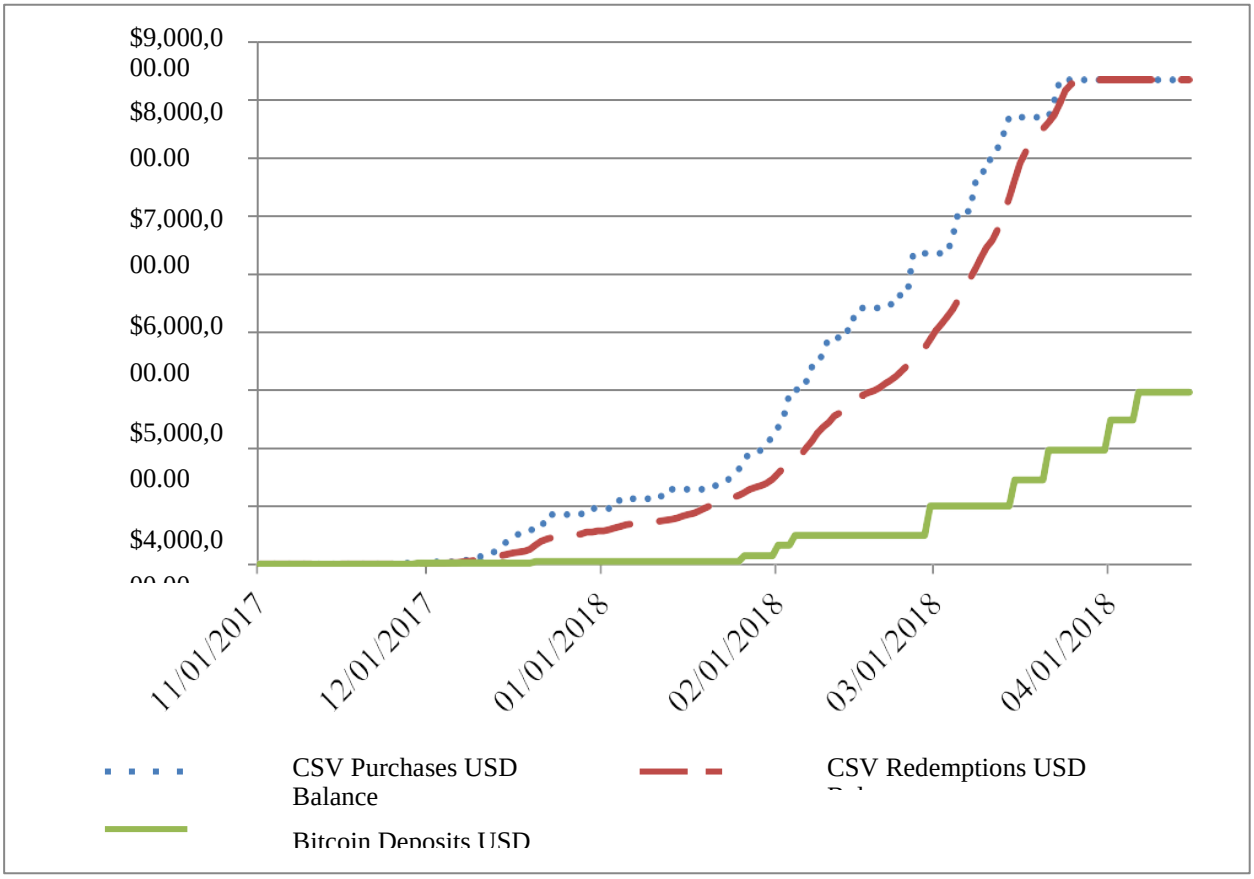
During the period of the fraud, Kvashuk gradually transferred about $2.8 million in cryptocurrency from his Coinbase bitcoin account to his bank and investment accounts. There is limited information about where the $2.8 million in bitcoin came from before it reached the Coinbase account, because Kvashuk used a "chipmixing" service that concealed the source of the bitcoin.

Kvashuk – who earned $116,000 a year at Microsoft – used this money to buy a $160,000 Tesla and a $1.6 million house in Renton. Kvashuk paid cash for the car and the house, with no financing.

As the chart below shows, Kvashuk's transfers from the Coinbase account to his

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

bank and investment accounts correlate with the timing of the theft of CSV, and the timing of the redemption of the stolen CSV. As more CSV was stolen and redeemed, more money flowed into Kvashuk's accounts. The cash deposits in Kvashuk's accounts are a percentage of the total value of the stolen CSV, which could be explained by fluctuations in bitcoin value, or by sale of the CSV at a discount.



Kvashuk did not report the $2.8 million on his tax returns. Records show that he told an online tax preparer that the money was a gift from his father – a Ukrainian civil servant who earns about $1,000 a month.

7/16/19 Search and Arrest

Kvashuk was arrested at his house on July 16, 2019. He made no statements. Agents are continuing to review devices and other evidence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Agents found over $4,000 in a purse belonging to Kvashuk's girlfriend. [redacted]

Agents found a notebook with what appears to be account information for numerous bank accounts in the names of various individuals and businesses. Kvashuk's girlfriend claimed, through counsel, that the notebook is hers. However, the girlfriend has refused to explain the contents of the notebook.

An agent found a handwritten note in Ukrainian at the house. A Ukrainian-speaking agent roughly translated the heading of the note as: "How I'm Going To Manage My Ten Million Dollars." The notes showed that Kvashuk planned to give some of the money to his father.

Recently Discovered Evidence

Since the detention hearing, agents have discovered critical additional evidence from seized digital devices. The search of these devices yielded what appears to be Kvashuk's "working file" for the fraud.

Exhibit 2 is an electronic document listing various critical information necessary to commit the fraud. Near the top is a list of "ms accounts," which includes at least two of the Microsoft online store accounts – pikimajado and xidijenizo – used to redeem stolen CSV. The middle part of the document refers to a "trade," "mixer1," "mixer2," and a "wallet." This appears to refer to the sale of stolen CSV to a third party, followed by movement of the bitcoin proceeds through two chipmixers, and finally the deposit of the proceeds in a bitcoin wallet. The bottom of the document lists the email addresses for the "avestu" and "sfwe2eauto" test accounts used to steal the bulk of the CSV, as well as what appears to be the login information for those accounts.

Exhibit 3 is multiple screenshots of confirmation emails sent by Microsoft in response to large-scale purchases of CSV from the online store. These screenshots

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

include the 5x5 code sequences (five blocks of five digits, separated by dashes) that a customer would need to enter in order to redeem the CSV at the Microsoft store and make purchases. In order to resell the stolen CSV, Kvashuk would need to provide the 5x5 codes to third-party purchasers. Some of these screenshots also show open browser tabs at the top, including open tabs for the "avestu" test account used to steal CSV.

Exhibit 4 appears to track numerous 5x5 codes stolen using the "sfwe2eauto" test account.

Exhibit 5 is a spreadsheet that appears to be an effort to organize and collate the tremendous number of 5x5 codes obtained as part of the scheme. The codes are organized into various categories by the type of gift card they relate to, such as $100 Windows store cards ("Windows 100") and $50 Xbox cards ("xbox50").

III. PROCEDURAL HISTORY

The detention hearing was held on July 19, 2019. The defense argued that there was little risk that Kvashuk would flee to the Ukraine because he fears persecution by the Ukrainian government, which led him to seek asylum in 2015. The defense also argued that the United States was merely speculating that Kvashuk might have unknown assets. The defense also contended that electronic monitoring and other conditions were enough to mitigate any flight risk.

Magistrate Judge Theiler rejected these arguments, finding that Kvashuk was an economic danger to the community and a flight risk. Exhibit 6, Transcript of July 19, 2019 Hearing at pp. 26-29. Magistrate Judge Theiler noted Kvashuk's incentive to flee given the danger of a long prison term, his ties to the Ukraine (contrasted with his lesser ties to the United States), the possibility of "significant" unknown assets, and Kvashuk's skill in anonymizing himself online. *Id.* Magistrate Theiler concluded that the proposed conditions of release -- although "pretty much the furthest we could go" -- would not "adequately" prevent Kvashuk from fleeing if he was "determined to avoid the charges." *Id.* at p. 29.

On July 24, 2019, the Grand Jury returned an indictment charging Kvashuk with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

one count of mail fraud in violation of 18 U.S.C. § 1341. The indictment alleged a scheme to defraud Microsoft out of $10 million in digital currency.

IV. ANALYSIS

As the defense notes, the standard of review by this Court is *de novo.* The record shows that Magistrate Judge Theiler correctly found that Kvashuk was a risk of flight, and that no conditions could adequately address that risk.[3]

A. Kvashuk Has Tremendous Incentive To Flee

Volodymyr Kvashuk is twenty-five years old. He has never been in trouble with the law, and until recently had a comfortable life, sharing his new waterfront home with his girlfriend and driving a Tesla.

Kvashuk's life was turned upside on July 16th, when armed agents raided his home, seized his phones and computers, and arrested him. The reality he now faces must be deeply frightening. Kvashuk is detained at the Federal Detention Center. He is charged with stealing ten million dollars, and trial is a little over two months away. If convicted at trial, his Guidelines range could be 87-108 months or higher. Kvashuk also knows that more charges are expected, including money laundering and tax evasion.

At the time of the detention hearing, the evidence was strong. Now, it is overwhelming. The agents found a note laying out how Kvashuk planned to spend his "ten million dollars." On Kvashuk's devices, the agents found Kvashuk's working file for the fraud – confirmation emails from Microsoft reflecting massive purchases of CSV, notes on the test accounts used to steal CSV, notes on accounts used to redeem the stolen CSV, and charts and spreadsheets used to track Kvashuk's growing inventory of stolen CSV and critical 5x5 codes. Exhibits 2-5.

This powerful evidence gives Kvashuk tremendous incentive to flee to his homeland, the Ukraine. Kvashuk grew up in the Ukraine, speaks the language, and has

---

[3] Magistrate Judge Theiler also found that Kvashuk posed an economic danger. Ex. 6 at pp. 26-27. Although the United States did not raise this argument, the massive scale and scope of the fraud, combined with Kvashuk's technical skill and ability to anonymize himself online, supports this finding.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

family there. His ties to the United States, on the other hand, are limited. He has only been in this country since 2015. He has no permanent status in this country. He may lose his job. Kvashuk claims to have applied for asylum, but success is far from guaranteed – especially given the pending criminal charges.

If Kvashuk goes to the Ukraine, he will be beyond the reach of U.S. law enforcement. Pursuant to the Constitution of the Ukraine, citizens of the Ukraine cannot be extradited to other nations from within its boundaries. CONSTITUTION OF UKRAINE June 28, 1996, art. 25.

The defense argues that Kvashuk would not flee to the Ukraine because he fears persecution by the Ukrainian government and has sought asylum in the United States. The merits of Kvashuk's asylum claim are beyond the scope of this proceeding. Nevertheless, as Kvashuk must know, there is no guarantee that his asylum claim will succeed, especially given the pending criminal charges. Kvashuk faces the very real possibility that he will be ultimately sent back to the Ukraine. Given that reality, Kvashuk might well decide to flee to avoid the risk of a long prison sentence in this country.

Furthermore, if Kvashuk truly fears a return to the Ukraine, he could flee to some other country, or within the United States.

B. The Evidence Suggests Kvashuk Has The Means To Flee

The defense claims that Kvashuk does not have "the financial ability to flee" because the United States has "seized or encumbered the vast majority of his assets." Although investigators have seized Kvashuk's *known* assets, the evidence suggests that he may have substantial unknown assets in any number of forms, including bitcoin or cash.

Although Kvashuk's counsel claims that Kvashuk has no other assets, Kvashuk himself would not confirm that to Pretrial Services. When interviewed, Kvashuk refused to make a meaningful financial disclosure. He would not say how he paid cash for the $1.6 million house or the $160,000 car. He would not say whether he had additional

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

bitcoin accounts. Kvashuk had every legal right to refuse to answer those questions – just as he would be within his rights to refuse to be interviewed by Pretrial Services at all. The result, however, is that the Court is deprived of important information.

The facts point to a very real possibility that not all the proceeds of the fraud have been recovered:

- Although Kvashuk stole $10 million in CSV, less than $3 million in proceeds have been identified;

- The note found in Kvashuk's house outlined his plans to spend "ten million dollars;"

- Kvashuk deliberately tried to erase the money trail by using multiple "bitcoin mixers;"

- Investigators have identified several bitcoin wallets that may be associated with Kvashuk, which in total contain bitcoin worth roughly $1.4 million. Kvashuk's connection to these wallets cannot be confirmed without further investigation.

- When Kvashuk's house was searched, agents found roughly $4,000 in his girlfriend's purse. [redacted] Kvashuk's girlfriend also claimed ownership of a notebook full of mysterious bank account information, but refused to explain these accounts.

The defense maintains that the United States "has not been able to dispel" the possibility that Kvashuk's wealth was a gift from his father. The evidence, however, refutes this theory. Records show that Kvashuk's father is a Ukrainian civil servant who makes roughly $1,000 a month. The financial analysis shows a close match in timing between the flow of money into Kvashuk's account and the time period of the fraud. Kvashuk's use of chipmixers show his intent to conceal the source of the money. The note detailing how Kvashuk would spend his "ten million dollars" showed that Kvashuk planned to give money *to* his father, which makes no sense if his father was the source of his wealth.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

[redacted].[4]

C. No Conditions Of Release Will Prevent Flight In This Case

Pretrial Services recommended release with conditions – a recommendation that Pretrial Services confirmed was driven by the restrictive criteria that governs its analysis. As just one example, Pretrial Services cannot consider the possibility that Kvashuk has failed to disclose all of his assets. Pretrial Services must also operate on the assumption that the traditional steps to mitigate risk – such as the surrender of Kvashuk's passport – will be effective, even though experience shows that defendants can flee despite such conditions.

This Court is not bound by the policies that constrain Pretrial Services. This Court can consider the totality of the evidence, and evaluate whether conditions such as electronic monitoring and passport surrender would *actually* prevent flight. The truth is that, if Kvashuk decides to flee, there are no conditions that will stop him.

As courts have repeatedly recognized, electronic monitoring has many uses, but it does not prevent flight. *United States v. Townsend*, 897 F.2d 989, 994-95 (9th Cir. 1990) ("Nor does the wearing of an electronic device offer assurance against flight occurring before measures can be taken to prevent a detected departure from the jurisdiction."); *see also United States v. Menaged*, 2017 WL 2556828, at *4 (D. Ariz. June 13, 2017) ("If Defendant intended to flee, the GPS device could easily be removed. The device would not prevent Defendant from traveling to another country. A GPS device would not prevent him from fleeing, and thus does not ameliorate his risk of flight."); *United States v. Patel*, 2017 WL 1098822, at *2 (E.D. Wash. Mar. 23, 2017) ("The Court further finds

[4] Investigators have found a bitcoin wallet that may be associated with Kvashuk titled "Dad Wallet." Tracing shows that bitcoin passed through chip mixers before being deposited in that wallet, which is inconsistent with the bitcoin coming from his father as a gift. In any event, the bitcoin in that wallet was worth less than $400,000, and thus only accounts for a fraction of Kvashuk's sudden wealth.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic home monitoring and GPS monitoring to be ineffective tools regarding the concern of flight, particularly foreign flight. When a monitoring device is removed or cut (which is what occurs when individuals flee), the Probation Officer receives an alert. However, there is no ability for the Probation Office to locate an individual and prevent them from departing the District or the country. These devices are more effective in addressing concerns related to safety of the community or other non-compliance.").

Seizing Kvashuk's passport is also no guarantee against flight. Determined fugitives regularly obtain documents or cross borders with no documentation. Kvashuk may even be able to get a new Ukrainian passport, by simply reporting that his current one was lost or stolen.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IV. CONCLUSION

For the reasons set forth above, this Court affirm the detention order.[5]

DATED this 19th day of August, 2019.

Respectfully submitted,

BRIAN T. MORAN
United States Attorney

/s/ Michael Dion
MICHAEL DION
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Phone: 206-553-7729
E-mail: Michael.Dion@usdoj.gov

[5] The United States does not plan to offer witness testimony at the evidentiary hearing. IRS Special Agent Eric Hergert will be available if the Court has questions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF SERVICE

I hereby certify that on August 19, 2019, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s).

/s/ Kylie Noble
KYLIE NOBLE
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-3903
Telephone: (206) 553-2520
Fax: (206) 553-4440
E-mail: kylie.noble@usdoj.gov